Caton

UNITED STATES DEPARTMENT OF COMMERCE
The Assistant Secretary for Communications and Information
Washington, D.C. 20230

May 25, 1994 90-314 1cB

The Honorable Reed Hundt
Chairman
Federal Communications Commission
1919 M Street, N.W.
Washington, DC 20554

Dear Chairman Hundt:

As you know, the Federal Wireless Policy Committee (FWPC), of which I am Chairman, was established last year to identify and evaluate wireless communications issues that affect the suitability of commercial wireless services and products for Federal Government users. Its members are a cross section of agencies that have operational, procurement or policy interests in the development of personal communications services (PCS) and other emerging new wireless services. The Federal Communications Commission has been represented in the meetings of the FWPC.

As a potentially large group of users of PCS and other commercial wireless services and products, federal agencies have a significant interest in the development of these services. One of the main objectives of the FWPC is to support the development of a digital, ubiquitous, interoperable, transparent and secure (DUITS) wireless communications network that can meet the federal government's operational requirements. In particular, federal users would benefit from systems that can be used easily in any part of the United States.

Enclosed for your information is a draft report of the FWPC's Requirements/Standards Subcommittee, titled "Current and Future Functional Requirements for Federal Wireless Services in the United States." This draft report, the result of two years of discussion and coordination in committees and at the Federal Wireless Users' Forum workshops, serves as a working guide for federal participants in the wireless technology development process. It identifies requirements of Federal Government agencies for emerging wireless services, both terrestrial and satellite-based, and raises issues regarding the ability of specific emerging wireless services to provide federal agencies with DUITS.

The draft report, approved by the FWPC at its April 29, 1994, meeting, has since then been presented to various standards bodies, including the Joint Technical Committee (T1/TIA), Committee T1/T1P1, and TIA Committee TR46. It will also be a part of a federal-industry dialogue at the next Federal Wireless Users' Forum on June 7, 1994, in Gaithersburg, Maryland.

Although a draft document, this report provides a good overview of the needs and concerns of federal users, and probably many other users, of PCS and other emerging commercial wireless services and products. The Commission's decisions in several rulemakings concerning emerging wireless services will, of course, be an important determinant of whether new commercial services will be able to meet the needs of Federal Government users. We hope that this report and its successors will help you and your staff in this very valuable undertaking.

Sincerely,

Larry Irving

Enclosure

cc: The Honorable Andrew C. Barrett
The Honorable Rachelle B. Chong
The Honorable Susan Ness
The Honorable James H. Quello

29 April, 1994

Current and Future Functional Requirements for Federal Wireless Services in the United States

I. INTRODUCTION

Federal government users of today's wireless communications services are especially aware of the impact Emerging Wireless Services (EWS), to include subscribed/leased commercial services or services interoperable with commercial services, will have on their future. The availability of cost efficient and universal EWS will enhance the effectiveness and productivity of many government agencies. Such advantages however will only be realized if EWS develops to accommodate the diverse national and international missions of the federal government. Federal user requirements are similar to those of state and local governments as well as the business community and should be given serious consideration in decisions affecting the future of EWS.

This document represents a summary of requirements from the anticipated federal users of commercially based wireless products and services. These services would include leased or subscribed services such as Cellular, Personal Communications Services (PCS), Mobile Satellite, and Enhanced Special Mobile Radio. It also includes products such as Wireless Local Area Networks (WLAN), Wireless PBX's, and Personal Digital Assistants (PDA's). These requirements reflect both licensed and unlicensed products and services. They also reflect some of the requirements for wireless products that might be customized versions of commercially available products to be used in private networks on government frequencies such as military or law enforcement application. This summary of requirements does not imply that the government user requirements are homogeneous and in search of a single solution. Rather, the federal user community is diverse. Many require less than the sum of all the requirements in this document. However, a common thread is found among the federal communities that reflects a clear set of needs that can be developed and articulated. This document intends to capture those common threads so as to guide government policy makers and industry planners in an acquisition strategy. These requirements are also intended to be submitted to appropriate standards bodies and industry organizations for consideration.

II. BACKGROUND

These requirements have been developed on the basis of recent policy decisions and trends in the federal government. A series of decisions in Congress and the Federal Communications Commission reflect a priority for the development and deployment of Emerging Wireless Services and the coincident migration from dedicated federal services on federal frequencies to usage on commercial leased or subscribed systems. The recent allocation of 160 MHz of spectrum for Personal Communications Services will be supplemented with the reallocation of 200 MHZ of spectrum from the government to the commercial sector. This reinforces existing policies to procure commercial off the shelf (COTS) products and services instead of custom products and government unique developments. This administration has placed a priority on the development of a National Information Infrastructure (NII) to support government, industry and the general public. EWS represents a key component of such infrastructure.

The requirements in this document have evolved from meetings and inputs from numerous government agencies beginning with the Federal Wireless Users Forum (FWUF), and including user workshops, and the Federal Wireless Policy Committee (FWPC) members.

The Federal Wireless Policy Committee was established in November 1993 with membership across federal agencies that have operational, procurement, or policy interests in the development of new Wireless Personal Communications Services and other emerging technologies. The FWPC is chaired by the National Telecommunications and Information Administration (NTIA) and vice-chaired by the Office of the Manager National Communication System (OMNCS). The FWPC serves the Assistant Secretary of Commerce for Communications and Information who is the principal advisor to the President on telecommunication policy.

The FWUF is a group of government wireless service users chaired by the OMNCS in response to tasking by the President. Its establishment followed from recommendations of the President's National Security Telecommunications Advisory Committee in their 5 September, 1992 Report. The FWUF sponsors workshops on federal wireless services that have supported the development of these requirements.

III. AREAS OF INTEREST

The following sections represent specific areas of interest in EWS as they affect federal users. Section A identifies the functional requirements that can be related to features and services in the EWS. Section B identifies issues related to the shared usage of spectrum. Section C identifies requirements and issues associated with security services.

A. Functional Requirements

The federal user requirements identified in this document encompass a broad array of user needs in the civil and defense agencies. Wireless services provided by EWS will enhance the performance and efficiency of day to day operations of law enforcement, drug enforcement, health & human services, defense, and countless other activities. These services will also play a significant role in disaster relief and crisis situations. These service requirements are generally characterized as Digital, Ubiquitous, Interoperable, Transparent, and Secure (DUITS), and are common to those of the business community with few exceptions. Users require voice, data, fax, paging and imagery services for diverse applications. Security features are required in most applications. Services should appear to the user to be universally interoperable and available using common devices with transparent operation. During periods of natural disasters and crisis it is especially important that EWS resources be available and readily configurable both nationally and internationally. These general requirements are expanded below.

A.1 Common Radio Characteristics

Ideally EWS would be supported by a single common air interface (CAI) for all services nationally and internationally. While the mix of new technologies, diverse radio channels and market dynamics make this "a hard problem" today, the federal user requires radio characteristics that can support services that are mutually compatible and can be made seamless to the user.

Within the large framework of possible access mechanisms addressed under the umbrella of EWS, some combinations of these are more important than others. The pairs of services below are thought to be those where seamless operation would be required. These paired services need not overlap and are not exclusive of other pairs that could be provided, e.g. satellite/point-to-point.

Paired Access Services (Voice & Data)	
Satellite	Cellular / Micro-cellular
Cellular / Micro-cellular	Wireless PBX
Wireless PBX	Cordless
Satellite	Point-to-Point (Land Mobile Radio)
Cellular / Micro-cellular	Point-to-Point (Land Mobile Radio)
Wireless PBX / Cordless	Point-to-Point (Land Mobile Radio)

Seamless operation for the above paired services would imply that they would have radio characteristics that are compatible and sufficiently common so that a common radio device would be practical to support paired services.

The aggregation of access mechanisms across multiple wireless networks as illustrated above characterizes the government's general needs for various types of geographic coverage. This should not be construed to mean that all government radios are required to span these media. Many government user applications will be accommodated by a single access mechanism.

A.2 Common Signalling

Common signalling mechanisms are essential if transparent access is expected under the umbrella of EWS. Where common signalling channels and protocols are not possible, automatic translation should be accomplished. This translation should be transparent to the application and the bearer services, terminal interfaces, and data related signalling.

A.3 Application Services

The EWS should support a set of application independent teleservices generally defined by layers 1-3 of the International Standards Organization's Open System Interconnect (OSI) model. As mobile services evolve it is expected that media independent applications will evolve to complement these teleservices. Independent of the wireless access mechanism, a minimum set of teleservices should be available to the user. While these services might vary with the bandwidth of the access service or an intervening network, service choices and protocols should be common. These applications are representative of federal user requirements but are not an all inclusive list.

These applications represent a mix of traditional circuit switched applications such as G3

Category	Application	Bearer Service
Circuit Mode	Voice	Voice
	Voice Band Data (V series)	Synchronous
	G3/G4 Fax	Synchronous
	Video	Synchronous
	STU-III	Synchronous
Interactive	Host/Terminal	Connection-Packet
	LAN Interactive	Connection-Packet
	Videotex	Connection-Packet
	Dial-up Services	Connection-Packet
Interactive	X-Windows	Connection-Packet
	Packet Voice	Connection-Packet
Transaction	Electronic Commerce	Connectionless Packet
	Identification Verification	Connectionless Packet
	Dispatch Services	Connectionless Packet
	Material Tracking	Connectionless Packet
	Telemetry	Connectionless Packet
	Vehicle Location	Connectionless Packet
	Vehicle Engine Diag.	Connectionless Packet
	Paging / Short Messages	Connectionless Packet
	Remote transactions	Connectionless Packet
Bulk Data Transfer	File Transaction	Connection-Packet
	Voice Messaging	
	G3 Fax	
	Message Service (X.400)	
Message Broadcast	Videotex	Broadcast Large Mess.
	Local Date/Time	Broadcast Small Mess
	Message Broadcast	Broadcast Large Mess.

Facsimile with new computer data applications such as X-Windows which will require teleservices that can efficiently adapt to each. It also includes non-traditional services such as Vehicle Location and Vehicle Engine Diagnostics with their own unique properties.

A.4 Network Services

As with the teleservices listed above a minimum set of network services should be available to the user of EWS. All of the above applications must be considered across the various network elements and interfaces to identify functions or properties necessary to support the service. The interaction of EWS and wired services should be complementary. The following are examples of some network services that should operate consistently across wireless and wired boundaries:

Transparent Interworking
Telecommunications Service Priority (TSP) system
Government Emergency Telecommunications Service (GETS)
Multilevel Precedence Preemption (MLPP) in private networks
Priority Access and Channel Assignment, PACA
PACA Override, PACAO
Personal Mobility
Terminal Mobility
In-Call Modification
Voice and Data Services
Bit Count Integrity for encrypted applications
Confidentiality
User Authentication
Signaling
User-to-User Signaling
Conferencing services
Off-hook, (ring down), services
Broadcast/Dispatch services
Universal access mechanisms
Handoffs between paired services

A.4.1 Transparent Network Interworking

Network interworking is closely coupled with many of the applications and is essential to support the service. The norm for early EWS will likely be an application that connects with non-EWS networks such as the Public Switched Telephone Network (PSTN), Integrated Services Digital Network (ISDN), or Packet Networks. Existing PSTN applications such as G3 Facsimile, STU-III and Point of Sale transactions are current PSTN applications that are supported by V series modems. These teleservices will require modem interworking as an integral component of the network services.

The teleservices identified above should be transparent to the user across a variety of wireless access networks and intervening wired networks. EWS G3 facsimile, for example, should operate transparently with modem based G3 facsimile on the PSTN. Network interworking should be provided to support transparent operation of wireless EWS with the PSTN, ISDN and with Packet networks. Specifically, the federal government as a potential customer of a EWS service would require the EWS be fully interconnected with the PSTN. Without full automatic interconnection, EWS would not provide the benefit that government users would require of this service, resulting in large government spectrum resources to provide wireless services to meet its needs.

A.4.2 Wireless Priority Treatment

As learned from several major natural disasters in the U.S., wireless communications capabilities (technologies) are essential in providing timely emergency telecommunications for the local, state and federal officials who are on-site and on the move under stressed environments. Wireless networks have, for example, provided a vital access to the PSTN bypassing locally damaged or disrupted landlines. However, due to the heavy traffic demand placed upon the surviving wireless systems, severe network congestions have been experienced, and resulted in high call blocking to the critical disaster relief officials when communications are needed the most. Therefore, future wireless systems should provide a uniform, nationwide priority access service to local, state and federal agencies during emergencies when local wireless networks become congested. A uniform, nationwide approach is needed to ensure effective implementation of the wireless priority treatment.Without a uniform, nationwide strategy, the implementation of different wireless priority schemes within and among regions may adversely impact critical operations. The implementation of the wireless priority treatment must be compatible with current and future local, state, and federal capabilities.

The priority treatment scheme should not preempt or affect calls in progress, but provide authorized priority users preferential treatment for any priority calls (i.e., voice, imagery or data attempts) via wireless networks. For the responsive and effective use of the priority scheme, it should be always available to authorized users without requiring a formal declaration of emergency. The priority scheme should be accessed by any authorized users on a standard terminal and become a part of the subscriber profile which will be recognized across the systems nationwide.

The following characteristics further define the wireless priority access requirements:
(a) Nationwide implementation approach to recognize priority users; One time transparent registration and access across networks (wired and wireless) for each authorized user;

> Identification and authentication of authorized users with a priority field in the user profile, such as High Probability of Completion (HPC) for the PSTN;
>
> Uniform nationwide service access including roaming with user profiles and service operation across various service providers;

(b) Nationwide system to assign priority users;

> Priority based upon the originating caller authorization, but invocable by the user through hardware and/or user verification;
>
> Priority for incoming calls to authorized users only from authorized users at origination;

(c) Transparency and Compatibility with the rest of the PSN;

> Transparent operation across handoff and service boundaries to the users through a single personal terminal and single number;
>
> Compatible with all other subscribed services;
>
> Future calls made through a wireless priority access scheme should be compatible with the Government Emergency Telecommunications Service (GETS) requirements, allowing the particular network and transmission paths to be

transparent to the users.

(d) Priority treatment defined, activated, administered, and invoked in a uniform manner consistent with TSP categories and criteria.

Priority access (forward) and egress (reverse) for radio channels through queuing of authorized call attempts when radio channels are full (PACA).Signalling/control access is assumed to be non-blocking or no-delay for authorized call attempts;

Multiple level priority treatment capability on a per call basis to authorized users;

Override of queued authorized user calls (per call basis) in accordance with multiple levels of priority for both radio and network resources (PACAO);

Enhanced routing of the wireless calls through diverse paths and alternate routing capabilities to get access into PSN or other networks when the normal routing is damaged or inoperable due to a damage during emergencies;

Exemption of the authorized user calls from selective network management controls that may be placed on the networks.

NOTE: PACA is generally described in TIA TR46 Services Descriptions consistent with these requirements for access. This service may change as it evolves into real systems.

The multi levels of priority access may be associated with specific qualifying categories and criteria. For example, the qualifying categories may include the following:

(a) National Security Leadership - This category will be strictly limited to only those telecommunication needs essential to national survival (e.g., Presidential communications, National Command Authority, Intelligence communications);

(b) National Security Posture and U.S. Population Attack Warning - This category covers those telecommunication needs essential to maintaining an optimum defense, diplomatic, or continuity-of-government posture before, during, and after crisis situations (e.g., conduct of diplomacy, command and control of military forces, space operations, continuity of federal government or state and local government functions supporting the federal government during and after national emergencies);

(c) Public Health, Safety, and Maintenance of Law and Order - This category covers the telecommunications needs for maintaining law and order and the health and safety of the U.S. population in times of any national, regional, or serious local emergency (e.g., law enforcement, continuity of critical state and local government functions, hospitals and distribution of medical supplies, critical logistic functions and public utility services);

(d) Public Welfare and Maintenance of National Economic Posture - This category covers the telecommunication needs for maintaining the public welfare and national economic posture during national or regional emergencies (e.g., Distribution of food and other essential supplies, Control of production and distribution of strategic materials and energy supplies, Transportation to accomplish the foregoing National Security/Emergency Preparedness (NS/EP) functions).

A.4.3 Priority Treatment in Virtual Private Network (VPN)

The preceding paragraph discusses wireless priority treatment in the PSTN. There is also a need for selected users (e.g., DoD) to have Multi-level Precedence and Preemption, Priority Access and Channel Assignment, and the Priority Access and Channel Assignment Override services available in order to support priority treatment in Virtual Private Networks. Standardization of these services will simplify efforts to achieve service transparency across multiple service providers of a VPN. Having MLPP defined as a standard does not automatically mean that it will be offered as a service in the PSTN.

(a) Description of MLPP Service - MLPP service applies in an environment termed a domain. Domains can be created by dynamic frequency partitioning or other means, and they may be variable or fixed in nature. An MLPP domain consists of a set of MLPP subscribers (MLPP users), the network, and access resources in use by that set of MLPP subscribers at any given time. Connections and resources that belong to a call from an MLPP user shall be marked with a precedence level and domain identifier, and shall be preempted only by calls of higher precedence from MLPP users in the same domain. Precedence provides preferred handling of MLPP service requests after the service requests are accepted by the system. It involves assigning and validating priority levels to the calls, and it also involves prioritized treatment of MLPP service requests (for example, in interaction with certain other services). Connections and resources belonging to calls from non-MLPP users and users from other domains shall not be preempted. (This service is ANSI and ITU-TS (formerly CCITT) standardized for the ISDN wireline environment.)

(b) Examples of Domains - A variable domain may be defined only in software in a private network with no particular number of channels (or circuits) assigned to the domain. The domain is initially inactive. When a call identifying itself as an MLPP call for a particular domain is attempted, a channel, if available, is assigned to that domain. In this process the domain is activated. Once the domain is activated and has one or more MLPP calls in progress, then additional MLPP calls may preempt the calls in progress. When the last MLPP call has ended, the domain once again becomes inactive.

The fixed domain would take a number of channels (or circuits) in the private network and designate them for use in MLPP service. With this kind of domain, the users of the service would always have some channels on which they could preempt. This type of domain could be used with a variable domain, which would handle overflow calls. In either case MLPP users only compete with each other for resources, not with non-MLPP users whose resources are unaffected once the domain is established.

A.4.4 Telecommunications Service Priority (TSP) and Government Emergency Telecommunications Services (GETS)

This section describes the existing government programs for access which are related to wireless priority issues. The TSP system for NS/EP was established by the FCC when it released a Report and Order (FCC 88-34) on November 17, 1988. The Report and Order established the TSP for NS/EP as an amendment to Part 64 of the Commission Rules and Regulations (title 47 CFR, Chapter 1). The Executive Office of the President has directed the Manager, NCS, to serve as the TSP system administrator. Details regarding service vendor's TSP system responsibilities are contained in the NCS's Service Vendors Handbook (NCS Handbook 3-1-2) which was approved by the FCC in a declaratory ruling on December 1, 1989.The President's National Security Telecommunications Advisory Committee (NSTAC) recommendations on the operation of TSP in wireless networks is available from the Wireless Services Task Force Report, Wireless Services for National Security and Emergency Preparedness (NS/EP) Communications (Draft dated 31 Jan, 1994).

GETS is the planned service to enhance the call access, transport, and egress with a nationwide switched voice and low-speed data communications service by utilizing the surviving PSTN resources. GETS calls will be afforded priority treatment and enhanced routing in the PSTN. GETS, which will be available nationwide, will provide domestic and international access and egress. User authentication will be provided using personal identification numbers (PIN) assigned to the authorized users. A new industry standard for the identification of priority calls as they travel through the PSN has been approved in the standard arena and is known as High Probability of Completion (HPC). The HPC definition will reside in the signalling messages of the authorized user calls and will.

A.5 Common User Interface

User interface for EWS devices should support a minimum set of common user interface features that will facilitate operation across the various EWS access networks and EWS devices. Examples include common keypad functions such as * and #, and common signalling such as "Operator" and "911" in accordance with the North American Numbering Plan.

A.6 Common Data Device Interface

The interface between EWS terminals and data devices should be limited to a common set of options defined by national and international standards, e.g., RS-232 standard for terminal connections.

A.7 Cost Efficient Service

Use of EWS by federal users is dependent on cost sensitivity of the service. Where multiple wireless access services are available, the least expensive access service should automatically be selected consistent with the user control or teleservices requirements.

B. Spectrum Issues

If the government users of EWS are limited to dedicated use of government allocated frequencies for government required services, then a larger allotment of spectrum will be required than currently exists. If government users are expected to share networks with commercial users as part of a network sharing agreement, these networks will be required to accommodate priority access schemes. This may be accommodated through separate or combined use of the services and features discussed in para. A.4.2, or their equivalent. Any sharing of services between government and commercial users would require that some combination of these services or features be an inherent part of EWS standards. Failure to accommodate some combination of these services or features into EWS would severely inhibit emergency services. Dynamic Variable Spectrum Partitioning may be one such equivalent method for accommodating these services and features.

Federal user requirements may be accommodated by a variety of spectrum allocation formulas. A solution for overall accommodation of federal requirements may include one or more of the following approaches.

Use of commercial services by lease or subscription

Use of EWS frequencies as a secondary government allocation to a primary non-government mobile application. An example of this is the government use of an ultra wide bandwidth CDMA system as an overlay to commercial spectrum on a non interfering basis.

The use of leased commercial systems on government frequencies.

The use of government owned systems on government frequencies.

The use of Dynamic Variable Spectrum Partitioning. An example of this would be the dedicated use of some bands for commercial use with the option for reallocation for government use in natural disaster or crisis situations.

If the government user is to share spectrum and services with commercial users their requirements as summarized above and in the security section that follows must be satisfied. In general the federal users need more than just voice service in one small region. Federal users require a minimum set of voice and data services that must interoperate across technologies, networks, carriers, and media boundaries. These services must be defined and supported by industry standards bodies.

If the government is to share spectrum with commercial users, the government may need to operate in bands for unlicensed services with commercial users. This would include both the government use of government owned commercial unlicensed (type accepted) equipment as well as modified commercial equipment to support government/military unique features. For example this would include commercial wireless (unlicensed) PBX's in government facilities or modified commercial wireless LAN equipment in military tactical applications.

Government services in a shared spectrum environment must be supported during restoration procedures in the event of disaster. Restoration of services may be supplemented by importing government radio systems on government frequencies.

C. Security Issues

Federal user requirements include a variety of security services common to the normal business user. These should be available in public EWS networks. Additional security requirements for federal users are identified as suited to private networks or supplied by the application. In any event, wireless networks should support user provided (application) security transparently through the network.A tabulation of federal user requirements for general use are shown below. These requirements apply only to the wireless components of the network.

FEDERAL WIRELESS REQUIREMENTS SECURITY SERVICES	Public Wireless Networks
Confidentiality	
Data Content	YES
Signalling	NO (see Note)
Addressees	NO (see Note)
Detection	NO (see Note)
Identification	YES
Geolocation	YES
Integrity: Accidental or Malicious	
Modification	YES
Insertion	YES
Deletion	YES
Destruction	YES
Replay	YES
Authentication	
Individual	YES
Device	YES
Network	YES
Availability: Accidental or Malicious Denial of Service	
Survivability/Recovery	YES

FEDERAL WIRELESS REQUIREMENTS SECURITY SERVICES	Public Wireless Networks
Priority Access	YES
ECCM[a] for malicious	NO (see Note)
Accountability	
Auditable	YES
Notarization	NO(see Note)
Non Repudiation	NO(See Note)

a. ECCM: Electronic Counter- Counter Measures, e.g. anti-jam capability.

Note: For certain DOD applications or in private US Government networks these confidentiality of signaling,addresses, and detection, and ECCM will be required. Notarization and Non Repudiation are value added features that may be added to some networks.

For USG classified or unclassified but sensitive applications additional security services, beyond those in the table, will be provided end-to-end independently of the network which supports them, e.g. STU-III service over PSTN.

A brief description of ISO defined security services follows:

Confidentiality - The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. This property also applies to locations and identities as users may be very sensitive to the idea of being tracked. The service is assumed to be applied to the radio channel of the wireless service.

Integrity - The property insures that data has not been altered or destroyed in an unauthorized manner.

Authentication - The process of verifying the identity of a user, terminal, or service provider to prevent fraud, abuse, and misuse of services.

Availability - The property of service being accessible and usable upon demand by an authorized entity. To augment emergency communications during and after a disaster or crisis situation, EWS needs a means to give government users priority use of resources and access to available services.This would also include provision for items such as emergency backup power.

Accountability - The property that ensures that the actions of an entity may be traced uniquely to the entity. Except for billing most of these services would be the responsibility of applications (end users).